# Course: Cisco IronPort Email Security Services

# Course WIFM

One of the daunting challenges that organizations face today is how to protect and manage the increasing volume of their email messages. Inbound messages can carry viruses, Trojan horses, and worms. These programs come under the generic term of malicious software referred to as malware. Outbound messages may carry sensitive business information or intellectual property.

With spammers and hackers on the rise, organizations need to protect their email systems with a well-integrated email security service that offers more than just malware protection, but also helps manage their email infrastructure effectively.

# Course Introduction

Welcome to the course on Cisco Hosted Email Security Services.
This course consists of three modules—Introduction to Hosted Email Security Services, Configuring Hosted Email Security, and Performing Day to Day Management. Module one gives you an overview of the Hosted Email Security services. Module two describes how to make configuration changes to Hosted Email Security and module three describes how to perform day-to-day management activities on your Hosted Email Security service.

# Course Objective

At the end of this course, you will be able to:

- Describe the Hosted Email Security services.
- Configure Hosted Email Security.
- Manage email reports.

# Module 01: Introduction to Hosted Email Security Services

# Module Introduction

Cisco IronPort is best known in the industry for its ESA Services. A couple of strategic investments have helped catapult Cisco IronPort towards industry leadership. These include SenderBase, a threat reputation service and Async OS, a purpose built operating system. Together, these have allowed Cisco to provide the best email security and consolidate multiple functions such as anti-spam, ant-virus, data loss prevention (DLP), and encryption onto a single platform, thereby offering customers maximum email security.

The Cisco IronPort Email Security services portfolio provides this industry leading technology in various form factors such as Managed Email Security, Hosted Email Security, and Hybrid Hosted Email Security. Based on their business needs, customers can choose the type of Email Security Service.
Managed Email Security provides remote monitoring and management of Cisco IronPort appliances that are deployed in the customer data center. In this deployment, Cisco can completely manage or co-manage the on premise email infrastructure.

In the Hosted Email Security deployment, the ESAs are located at Cisco data centers and provide customers with security as a service delivery option. This offering provides dedicated infrastructure to customers in addition to all the advanced features available as part of the ESA. This saves the customers the need to deploy an email security infrastructure and thereby avoid excess staffing and capital overheads.

Hybrid Hosted Email Security provides customers with maximum flexibility of a hosted offering along with the control of outbound mail provided with on-premise equipment. In this deployment, customers typically use the hosted infrastructure for spam and virus filtering on the inbound mail, and use the on-premise equipment to protect organization-specific information through solutions such as DLP and encryption.

# Module Objectives

Welcome to the module on Introduction to Hosted Email Security Services.

At the end of this module, you will be able to describe the Hosted Email Security services, the methods for stopping email malware, the tools used to manage the email infrastructure, the hosted services network topologies, and also describe the Cisco IronPort Email Pipeline.

# Lesson 01 - Overview of Hosted Email Security Services

## Cisco IronPort Hosted Email Security Services

Hosted Email Security services include spam protection, content filtering, virus defense, email authentication, message tracking and reporting.

## Cisco IronPort Hosted Email Security Services Architecture

Customers can route their email messages through the Cisco IronPort Hosted Email Security solution for content filtering. The Cisco IronPort Hosted Email Security solution cleans up all inbound mail by using industry leading anti-spam, anti-virus, and other rules. This ensures that the mail traffic that reaches the customer premises is free from email malware. On the outbound, customers can either send their email from the mail server for delivery to the next hop or pass it through the Cisco IronPort for filtering, footer stamping, and other services.

The dedicated customer email infrastructure is monitored 24 x 7 by Cisco security specialists located at Cisco Security Operations Centers (SOCs). The SOCs host service desk capabilities to answer support related questions and also hosts a comprehensive support portal that provides customers visibility about the health of their email infrastructure.

This implementation acts as an early detection system that provides Cisco security analysts the visibility required to provide the highest level of service to the customer. So, in a sense, you are getting a Service Level Agreement (SLA)-backed email security solution based on an industry-leading dedicated infrastructure. Besides a dedicated infrastructure, you will also get future capacity assurance. Cisco IronPort will provide all the necessary hardware, software, and bandwidth required to deal with increased volumes of spam.

The Cisco IronPort Hosted Email Security services portal offers easy access to your email administrator for configuring these changes. You can access any quarantined mail, reporting data, or email messages aggregated across both the ESAs. You can also search for a single email based on sender, receiver, or time parameters through the message tracking option.

## Features of Cisco IronPort Hosted Email Security Services

The Hosted Email Security solution offers several features that provide you maximum email security. The following table describes the various features of Hosted Email Security solution.

| Feature | Description |
|---|---|
| Dedicated infrastructure | • Ensures maximum data protection<br>• Ensures that the customer's mail infrastructure is highly available<br>• Ensures protection of sensitive business information by using Content Filters<br>• Provides advanced controls such as email authentication and Transport Layer Security (TLS) |
| Capacity assurance | • Includes the necessary hardware and software to control large volumes of spam<br>• Saves the customers additional costs on purchase of new hardware to control spam |
| Spam protection | • Includes Cisco IronPort Reputation Filters to perform an assessment of email security threats<br>• Offers protection from the widest range of known threats with industry-leading accuracy by using Cisco IronPort Anti-Spam |
| Virus protection | • Provides a multi-layered, multi-vendor approach to virus filtering<br>• Offers the first line of defense by using Cisco IronPort Virus Outbreak Filters for detecting and stopping viruses<br>• Uses Integrated McAfee or Sophos anti-virus technology for maximum protection against the most complex virus attacks |
| 24 x 7 monitoring and support | • Ensures maximum uptime of the email infrastructure<br>• Ensures that email security is always available through multiple data centers working round-the-clock |

# Lesson 02 - Overview of Cisco IronPort Hosted Hardware

## Types of Cisco IronPort Hosted Hardware

The Hosted Email Security deployment includes two types of email security hardware—the ESA and the security management appliance (SMA).
Email security hardware (ESA) is an email gateway that offers a multilayered approach to email security—providing advanced threat prevention, blocking spam and viruses, and enabling corporate data loss prevention.
Security management appliance (SMA) is a platform for managing all policy, reporting, and auditing information for the ESAs.

## ESA Features

The ESAs continually receive updates from Cisco IronPort to offer real time protection against email security threats. You can configure ESAs to handle outgoing mail. This allows you to scan all outgoing email with Content Filters that search for key words in email messages or in attachment, thereby ensuring that sensitive business content is protected.
By default outgoing email will bypass the hosted services hardware so outgoing email can not be scanned, unless the hosted customer requests their mail server point to the hosted hardware.

## SMA Features

The SMA helps you consolidate reports from multiple ESAs configured in the network. You can also view reports on individual systems. You can consolidate message tracking. You can also track a message regardless of which appliance it passes through.

You can integrate the Spam Quarantine feature into the existing directory and mail systems. If end users need to quarantine suspect spam, the SMA provides a centralized storage that allows customers to access and determine the appropriate action. Therefore, customers' mail servers do not have to store spam.
The SMA supports advanced message tracking. This allows email administrators to know the final disposition of the email and when it took place. The message tracking data of the two ESAs is aggregated together onto the SMA so that the disposition of a single email can be determined, regardless of its original path.

# Lesson 03 - Overview of Hosted Services Network Topologies

## Network Topology of Cisco IronPort Hosted Email Security

Now that we know about the hardware, let's discuss how the hosted hardware fits into the hosted services cloud. In a Hosted Email Security deployment, all the email security hardware is located in the Cisco IronPort Hosted Email Security cloud. The incoming email is load balanced against the ESAs that make up the cluster. At least 90 percent of the email traffic is filtered out and the remaining clean mail is forwarded to the end users Inbox.

Preventing the delivery of email to invalid recipients usually requires recipient validation against a Lightweight Directory Access Protocol (LDAP) server by an on-premises gateway appliance. The hosted ESAs use a method called Call Ahead to contact the LDAP server before forwarding the message.

The SMA collects the reporting and tracking information on these activities along with suspect spam. By default, outbound email is sent directly from your groupware server to the Internet. You can route the outbound mail sent back through the clusters and decide on the appropriate content filters. The controls for making these changes are available to your email administrator through the Cisco IronPort Hosted Email Security Services portal. You can access any quarantined mail, view reporting data or email aggregated across both appliances, or search for email based on the sender, recipient, and time by using the Message Tracking option.

## Network Topology of Cisco IronPort Hybrid Hosted Email Security

In the Cisco IronPort Hybrid Hosted Email Security deployment, an ESA is placed at the customer premises. Similar to the Hosted Email Security deployment, the ESA in the Cisco data center cleans up all messages before forwarding it to the customer network. However, the on-premises appliance will receive and forward the email traffic to the groupware server. The on-premise ESA allows for more flexibility. For example, the ESA allows the customer to perform LDAP group lookups on outbound mail. This is critical for deciding which user groups will be encrypted or if they require custom footers that are group-dependant.

Because the nature of the configuration of the outgoing mail for on-premises appliances can vary widely, from one hosted customer to another, the email administrator at the customer site is responsible for maintaining the on-premise appliance.

This training will not prepare you for performing these tasks. Please consult our training page to access the Instructor-led courses. In our online catalog, look for convenient dates and locations for Securing your Email, Parts 1 and 2.

# Lesson 04 - Cisco IronPort Email Pipeline

## Email Security Appliance Filters

The ESA consists of individual filters that are collectively referred to as the Cisco IronPort Email Pipeline.
The following table describes each type of the filter of the Cisco IronPort Email Pipeline.

| Type of Filter | Description |
|---|---|
| Reputation Filters | First, the Reputation Filters block email messages from suspicious sources. The Reputation Filters use SenderBase Reputation Service (SBRS) for protecting legitimate senders from spam. The SBRS blocks IP addresses from unsolicited commercial email messages and allows only legitimate email traffic to enter the customer premises. |
| Anti-Spam | The Anti-Spam filters then perform a detailed analysis about these details: the sender, the type of content, and the message structure, besides detecting spam. The Anti-Spam filter blocks spam attacks before they slow down or impact customer network. This filter removes unwanted mail before it reaches the customers inbox, without violating user privacy. |
| Anti-Virus | Then the Anti-Virus filter scans the email traffic for viruses, Trojan horses, and worms.<br>The Anti-Virus filter offers the choice of enabling two anti-virus scanning engines—Sophos and McAfee. These two engines scan messages and attachments for viruses on a per mail policy basis to prevent email malware from entering customer network. |
| Content Filters | After virus and spam has been filtered, Content Filters remove particular file types as chosen by the customer before passing the email traffic on to the virus outbreak filters. The Content Filters scan both inbound and outbound mail traffic. Filtering outbound mail traffic helps protect confidential or inappropriate information from entering or leaving customer premises. |
| Virus Outbreak Filters (VOFs) | The VOFs feature includes special filters that provide a first layer of defense against new attacks. Messages containing file types that have suddenly increased in numbers across the email community are automatically sent to a quarantine named Outbreak. These are then processed according to newly updated VOF rules. Subsequently, the quarantine releases the email messages for delivery or sends the email messages back to the Anti-Virus filter for rescanning. |

# Module Summary

Now that you have completed this module, you will be able to:

- Describe the Hosted Email Security services.
- Describe the methods to stop email malware by using hosted ESAs.
- Describe the tools for managing the email infrastructure.
- Describe the hosted services network topologies.
- Describe the functionality of the Cisco IronPort Email Pipeline.

# Module 02: Configuring Hosted Email Security

# Module Introduction

Welcome to this module on Configuring Hosted Email Security.

In this module, you will go through configuration changes that can be applied to the hosted ESA.
Using the Cisco IronPort Hosted Security Services portal, you can manage ESAs and SMAs by accessing the ESA user interface and the SMA user interface, respectively. Your hosted ESAs have been grouped into clusters to manage both appliances at the same time.
Accessing the ESA cluster allows you to control Simple Mail Transfer Protocol (SMTP) connections by using mail flow policies. For example, you can unblock a preferred sender, edit the Host Access Table (HAT) by using mail policies, and add friendly domains.
You can create custom filters for your email messages. In addition, you can change the quarantine suspect spam by making configuration changes to the C-Series cluster.

# Module Objectives

At the end of this module, you will be able to describe the administration of the Hosted Email Security system, how to control SMTP connections, how to use Anti-Spam, how to administer Content Filters, and also describe how to administer Cisco IronPort Spam Quarantine.

# Lesson 01 - System Overview

## Management Access to Your Hosted Hardware

To access the security management appliances via the GUI, click the Network Details tab and then click the Devices tab. Notice that the device is listed in the **Devices** list. Next, in the Devices list, double-click the device that you wish to manage. For example, SMA1.

To manage the device, select the device, and then click **Open Admin Console**. The browser to the Web-based Management Interface of the selected device will open.

Now that you know how to access the web based management of your portal hardware, let's look at the GUI of an ESA.

The Web-based Management Interface contains several options for managing ESAs. Let's focus on the options used to manage a hosted environment.

The **Monitor** tab contains various email reports that you can view. Because you are logged into the ESA interface, reports will not account for the mail that is aggregated across all appliances. To view the aggregated report, you must log on to the SMA interface.

The **Mail Policies** tab contains the **Host Access Table (HAT)** and the **Recipient Access Table (RAT)**. The HAT controls Simple Mail Transfer Protocol (SMTP) conversations by categorizing email domains based on their reputation. The RAT limits the forwarding of email messages only to domains inside the organization.

Using the **Mail Policies** option, you can define the filters to be applied to the email traversing the work queue. You can define content filters for both incoming and outgoing email.

You can use the **Trace** option on the **System Administration** tab to create a fictitious email to verify whether the fictitious email is permitted or blocked by the security filters. This helps you predict the affect of configuration changes before committing them to the production mail flow.

You can view the online documentation that pertains to the current management menu by clicking the **Online Help** tab.
You should not change certain configuration changes. These configuration settings are prefixed with Remote Management (RMS).

## What Are ESA Clusters?

Since the ESAs are grouped into a cluster, you can manage and configure multiple appliances at the same time, reducing administration time and ensuring a consistent configuration across your network.

To access your cluster, select the ESA cluster in the devices column. Enter the logon credentials, and then select the level to manage the appliances at. There are three levels: Cluster, Group, and Machine.
If you select the Cluster or Group level, the configuration changes that you execute will be applied to all ESAs.
If you select the Machine level, the configuration changes will be applied only to that particular machine.

## The SMA User Interface

You can also access the SMA interface through the Hosted Security Services portal.

You can use the **Monitor** tab to generate reports on several categories of email. Because the data for the reports is aggregated from the cluster, the time taken to generate the reports may be longer.

Using the **Email Data Availability** option, you can check on how current the reporting or message tracking data is.

The **Spam Quarantine** option allows you to view the email quarantined at the cluster and stored in the SMA.

The **Message Tracking** option allows you to track the status of individual emails that have traversed through any of the ESAs.

You can view the online documentation by clicking the **Online Help** tab.

# Lesson 02 - Controlling SMTP Connections

## Process of Email Delivery

The process of delivering an email through the Cisco IronPort Hosted Security Services cloud begins with a remote mail server connecting to the ESA on Port 25. During the TCP connection, the ESA verifies the reputation of the sending domain's IP address at Cisco IronPort.

For example, Mark from outside.com sends an email to Harry at exchange.juliet.com.
When outside.com initiates an SMTP connection, the ESA verifies the domain's reputation. By default, HAT is programmed with a range of reputation scores for every sender, and also has corresponding mail flow policies. Outside.com has a score of -2.7. Therefore, it is placed in the Suspect list and the THROTTLED mail flow policy is applied to the email messages received from this domain.

The next stage is to check if the recipient domain is defined in the Recipient Access Table (RAT). If the recipient domain is not defined in RAT, the email will be rejected. In this example, recipient domain, exchange.juliet.com is defined in RAT. Therefore, the email from Mark is accepted by Harry at exchange.juliet.com and the SMTP connection will be closed.

## Mail Flow Policies

HAT associates the sending domain's IP address with a sender group based on its reputation. Then, the mail policy associated with that sender group is applied to email received from that domain. The Mail Policies table defines the actions taken in each mail policy.

For example, since the THROTTLED mail flow policy is applied to email messages from outside.com, the number of email messages received from outside.com is limited to 20 messages per hour. In addition all email messages from outside.com will be scanned by the Anti-Spam and Anti-Virus engines, and by Virus Outbreak Filters. Note that all mail flow policies apply the Anti-Virus engine.

However, the TRUSTED and RELAYED mail flow policies will not apply the Anti-Spam engine. If a particular domain is in the White list sender group, the TRUSTED mail flow policy will be applied and the Anti-Spam engine will be skipped.

## How to Unblock a Preferred Sender

There may be instances where domains that send you business email have a poor reputation score. For example, the NewBP.com domain has a reputation score of -4. This falls into the Black list whose range is -10 to -3. Therefore, the domain receives a reject notification and the SMTP connection is closed. A temporary solution is to add the NewBP.com domain as a friendly domain.

## How to Add Friendly Domains

To add NewBP.com to the WHITELIST, you must first select the “Mail Policies” tab and scroll down to “HAT Overview” option. You must then click on the WHITELIST hyperlink.

On the Add Sender to WHITELIST – IncomingMail page, specify the sending domain that needs to be white listed. Add the host domain, in this example, NewBP.com. Alternatively, you can add classless interdomain routing (CIDR) ranges.

Ensure that you document the changes before submitting. You can add comments on this configuration page, or later at the global commit. The messages received from NewBP.com will not be checked for spam.

## How Committing Changes Affects Mail Flow

As you make configuration changes, click the **Submit** button on each page to commit the changes. Alternatively, you can commit all the changes globally by clicking the **Commit Changes** button. The documentation page is displayed. You can either abandon or commit the changes. You can also add comments and then commit the changes to the mail flow. The comments are added to the mail log along with the administrators name and the date on which the comment was entered. After you commit these changes, all changes will be applied to the production mail. After you commit the changes globally, the **Commit Changes** button will be disabled. This indicates that there are no pending changes.

# Lesson 03 - Anti-Spam and Anti-Virus Administration

## Anti-Spam Protection in the Work Queue

In the work queue, the Reputation Filters and the Anti-Spam engine work together to remove the incoming spam. The Anti-Spam engine handles email from domains that have an acceptable reputation score, but are still sending out spam. The Anti-Spam engine has a separate rating system for separating clean mail from spam mail.

## Spam Analysis

Based on the spam analysis, a score between 1 and 100 is assigned to the mail. Suspect spam is email with a score between 50 and 89. Positive spam is email with a score of 90 or above, and all other email messages are certified as clean.
Every five minutes, the Cisco IronPort Anti-Spam downloads a new rule set. The engine is designed to take a look at four main data points. These are Who, How, What, and Where. Analyzing each of these points determine a weight. The sum of these weights determines the spam analysis score.

The following table describes how to analyze the data points.

| Data Point | Analysis |
|---|---|
| Who | • Check out the sender's IP address.<br>• Identify the regions that have a reputation for sending spam.<br>• Look for email messages from those regions. |
| How | • View the construction of the message.<br>• Check out if the message has been constructed by using an unbranded software application. |
| What | • View the message content.<br>• Check out if the image contains random dots.<br>• Check out if the image contains the same color scheme received several times by the Cisco IronPort spam traps. |
| Where | • Check out where does the URL in the spam takes you.<br>• Check out if the URL takes you to a Web site with a low Web reputation. |

## How to Configure Mail Policy Anti-Spam Settings

By default, the Anti-Spam engine for Cisco IronPort Hosted Email Security is set to drop positive spam and deliver suspect spam.

These settings do not allow for any quarantining. If your end users need to have their suspect spam quarantined so that they can access it later for a final decision, then you need to change the anti-spam settings to from forwarding suspect spam to quarantining suspect spam. Since all of the incoming email passes through the default mail policy, all of your end users spam will have their suspect spam quarantined.

For example, change the default policy and configure the anti-spam setting to pick specific users to have their suspect spam quarantined, and have all others delivered or dropped.

To change the default policy, click the hyperlink in the Anti-Spam column. On the Mail Policies: Anti-Spam page, quarantine all of your suspect spam. Alternatively, you could change the subject tag for suspect spam, or add an X-Header, that is tied to a Microsoft Office Outlook rule if you want to force the suspect spam into an Outlook Junk Mail folder. To enable a second anti-virus engine, on the **Security Services** tab, click **McAfee**, and then accept the license agreement.

## Anti-Virus Protection in the Work Queue

The Cisco IronPort Anti-Virus system has two filters: the Sophos Anti-Virus engine and the McAfee Anti-Virus engine. The Sophos Anti-Virus engine uses signature matching, heuristics, and a launch of executable files to determine if an attachment is virus infected. You can also enable a second Anti-Virus engine from the anti-virus vendor, McAfee.

If the attachment contains a virus that has just been released and there is no signature for it, then the Anti-Virus engine will not detect it, and the email is forwarded down the work queue. Virus Outbreak Filters are designed to address this newly created virus.

The email appliance receives updates every five minutes regarding a surge in particular file types distributed through email. Virus Outbreak Filters will catch email messages whose attachments match these types, and quarantine them until updates are received that discern the threat.

When the virus signature is published, the quarantined email messages are re-scanned and released or deleted.

## How to Configure Mail Policy Anti-Virus Settings

To change the Anti-Virus engine settings, click the **Mail Policies** tab, click **Incoming Mail Policies**, and then click the hyperlink in the **Anti-Virus** column. Notice that the default mail policy contains the default anti-virus settings. Incoming files that are encrypted or are too large to scan within 60 seconds are delivered. A subject tag is added to the email to indicate to the end user that the email was not scanned for virus.

On the Mail Policies: Anti-Virus page, you can configure mail policy anti-virus settings. For example, you can choose to quarantine encrypted messages or delete them. You need to repair the attachment that contains a virus.

# Lesson 04 - Managing Content Filters

## Scenarios for Using Content Filters

The anti-spam and anti-virus defense mechanisms are designed to address general email threats. However, if your email requires a custom filter in addition to the protection provided by the Anti-Spam and Anti-Virus engines, then Content Filters can be used to address this need. For example, you may need to delete executable files, or set a maximum attached file size.

Content Filters are a set of conditions and resulting actions. They act either on the content or on the mail headers to classify, accept, or reject a message.
Here is a partial listing of some of the combinations that can be performed. The criteria list represents the conditions and the actions list represents the actions you can take.

## Content Filter Configuration Process

When you build a filter, first, you need to recognize the content that needs a custom action. Next, open the **Filter** menu, and select the conditions and actions that match your choices. Then, select a mail policy to apply the content filter. Next, test the filter by using the Trace tool. After you are satisfied with the result, commit your changes globally.

## How to Create a Content Filter

You can create content filters by using the Incoming Content Filters page.

To access the Incoming Content Filters page, on the **Mail Policies** tab, click **Incoming Content Filters**, and then click **Add Filter**. On the Add Content Filter page, specify the filter name and a description for the filter. It is recommended that the filter name you provide reflects the action to be taken on the email.

Next, specify the matching criteria for the content filter. To do this, click **Add Condition**. In the Conditions list, select a condition, and then click **OK**. You can add multiple conditions to a filter.

Next, specify the action to take on email that matches the criteria. To do this, click **Add Action**.

In this example, the condition is to look for the string "Confidential". If there is one occurrence in the body of an email, the action is to quarantine the email to the policy “Quarantine”. After selecting an action, click **Submit**.

Next, apply the content filter to an incoming mail policy. To do this, on the **Mail Policies** tab, click **Incoming Mail Policies**. View the default mail policy. Note that no content filters are enabled for the policy. You need to enable content filtering for the policy. To do this, on the Mail Policies: Content Filters page, click **Yes**. Next, click **Enable** to specify the filter to apply to the policy, and then click **Submit**.

Notice that the content filter you created is listed under the **Content Filters** section. The content filter will be applied to the production email only if you click **Commit Changes**. It is recommended that you test the filter operation by using the Trace tool before committing the changes globally.

### How to Test Filter Operation with Trace

You can test filters by using the Trace tool. The tool emulates a message as being accepted, and prints a summary of features that would have been "triggered" or affected by the current configuration, including changes that have not yet been committed.

Notice that we have placed the word "Confidential" in the body of this fictitious email. To test the filter, click **Start Trace**. The trace output indicates that the filter would have been trigged and the quarantine action executed against this email. The best practice is to run the Trace tool against several positive samples and several samples that should not result in action.

After you are satisfied with the performance, commit the changes to the production email by clicking **Commit Changes**.

## Module Summary

Now that you have completed this module, you will be able to:

- Describe the administration of the Hosted Email Security system.
- Describe how to control SMTP connections.
- Describe how to use Anti-Spam.
- Describe how to administer Content Filters.
- Describe how to administer Cisco IronPort Spam Quarantine.

# Module 03: Performing Day to Day Management

# Module Introduction

Welcome to the module on Performing Day to Day Management.

A large percentage of an organization's incoming mail is either spam or virus. You can provide data security through a hosted Security Management Appliance (SMA) that allows you to review email tracking and reporting data that describes the present as well as the archived reports. Using the management appliance, you can access reports on incoming mail and internal users, as well as track individual messages.

# Module Objectives

At the end of this module, you will be able to:

- Describe the features of the Email Security Monitor.
- Describe how to access the Incoming Mail report.
- Describe how to access the Internal Users report.
- Describe how to track messages

# Lesson 01 - Using Email Reports

## Email Security Monitor

The Email Security Monitor feature in the management appliance is a real-time threat monitoring and reporting system that is integrated into every IronPort SMA. By using the Email Security Monitor, you can review email reporting and tracking data that describes the present and archived reports. This helps you identify the source of Internet threats such as spam, viruses, and denial-of-service attacks, and manage email messages and internal users.

## How to Access the Incoming Mail Report

To access the Incoming Mail page, on the **Monitor** menu, select **Incoming Mail**. The Incoming Mail page provides access to the real-time activity of all public listeners configured on your ESAs.

The Incoming Mail page consists of two main sections: Mail Trend Graphs and Incoming Mail Details. The Mail Trend Graphs section summarizes the top senders by total threat messages and by total clean messages received from them. The Incoming Mail Details section allows you to view domain details such as the IP addresses, or network owners, based on the view configured. You can sort the column data by clicking the column headings.

## How to Access the Internal Users Report

To access the Internal Users page, on the Monitor menu, select Internal Users. The Internal Users page provides information about the email sent and received by internal users per email address. A single user can have multiple email addresses. The email addresses are not combined in the report.

The Internal Users page displays graphs of top users based on the total number of clean incoming messages and clean outgoing messages, and the User Mail Flow details. The User Mail Flow Details section displays details such as the number of spam messages and clean messages detected. You can generate a report for a time range such as day, week, month, or year. You can also export the graph data or the details listed to CSV or PDF format by clicking the **Export** link.

Note that by default your hosted appliance will not be able to monitor email from internal users unless you have configured outbound mail to travel through the security services cloud.

## How to Track Messages

To access the Message Tracking page, on the **Monitor** menu, select **Message Tracking**.

You can use the Message Tracking page to quickly determine the exact location of a message. This avoids the need to search through log files.

You can search for a single email based on the four categories—Envelope Sender, Envelope Recipient, Subject, and Time period of receiving message.

You can also perform an advanced search for messages based on four categories—Sender IP Address, Virus Positive, Suspect Spam, and Hard or Soft bounced.
For example, you can search for all email sent to a recipient for a time range. You can view the message details by clicking the **Show Details** link. You can view the results returned by the security engines for the email. In this example, the verdict of the anti-spam engine is negative but the verdict of anti-virus engine is positive.

## Module Summary

Now that you have completed this module, you will be able to:

- Describe the features of the Email Security Monitor.
- Describe how to access the Incoming Mail report.
- Describe how to access the Internal Users report.
- Describe how to track messages